www.bell.ca

Prepared by: Bell Canada
PWGSC: W7714-08F01
CSA: Daniel Charlebois

Bell Canada
160 Elgin Street
17th Floor
Ottawa, Ontario
K1S 5N4

Secure Access Management for a Secret Operational Network (SAMSON) Technology Demonstrator (TD), SD006 Trial Report Phase II (2011)

Empire Challenge (EC) / Coalition Warrior Interoperability Demonstration (CWID)

Version: Final

15 August 2011

DRDC-RDDC-2014-C31

Bell

This document does not include sensitive information. Instead, this document may contain external references to separate documents containing sensitive information. This allows this document to be unclassified, as any classified, protected or proprietary information is referenced, not disclosed.

The SAMSON TD system is being designed to not be a classified system. The SAMSON system will provide access to sensitive information, but the system itself is designed to be unclassified. The SAMSON configuration data (such as specific user access control parameters and related security controls used in the Policy Decision Point algorithms) for a specific instance is sensitive information, and appropriate safeguards are provided to protect this data.

Contents

1 DESCRIPTION

This report describes the planning and execution of two independent trial activities that constituted the completion requirements for the phase II SAMSON TD development effort. These demonstration activities includes:

- Empire Challenge 2011 (EC2011): Empire Challenge is an annual US joint military and coalition intelligence interoperability demonstration. It is hosted out of Fort Huachuca, Arizona with connectivity provided through JFCOM to link demonstration partners including DRDC Shirley's Bay. The goal of the demonstration is to deploy new technologies into a simulated operational environment. (May 9 - June 3, 2011)
- Coalition Warrior Interoperability Demo (CWID2011): CWID is a global interoperability event that allows for the discovery of leading edge C4ISR technologies to identify and fill warfighter and agency gaps. (May 30 - June 24, 2011)

Both trials shared a common objective to improve information protection and access management for military and defence operations on SECRET networks in order to provide application independent caveat separation of information for use in common operational picture correlation and reporting in a federated multinational information sharing environment. Both trials were conducted using a common defined scenario that exercised the core phase II SAMSON capabilities. Both trials were successfully completed with all technology and capability targets achieved.

2 TRIAL DETAILS

Both trials leveraged a common technology implementation and shared a common set of scenarios and test cases. The focus of the information presented in this section relates primarily to the CWID trial as because:

1. the CWID working groups required a more formal scenario development process for SAMSON involvement in the trial; and
2. the CWID trial was conducted by an independent set of operators and thus provides a more objective opinion of SAMSON capabilities.

2.1 TEST ITEMS

The following list of software components were used in the EC2011 and CWID2011 trials. This list reflects the software that was relevant to the definition of the trail scenarios.

2.1.1 WORKSTATION

- OS: Windows 7 Professional
- Office Suite: MS Office 2007
- Email: Outlook 2007
- IM Client: Transverse 1.5.4 (with the SAMSON client plugin)
- Titus Labelling Software 3.0.1 (document, email and generic file labelling)
- Geospatial Applications: Google Earth 5.0, GeoViewer 3.0

2.1.2 BACK OFFICE SERVERS

- Domain Controller: Windows 2003 Server with Active Directory
- Mail Server: Windows 2003 Server with Exchange 5.5
- File Server: CentOS 5 with Samba3
- Instant Message Server: CentOS 5 with Openfire 3.7

2.1.3 SECURITY SERVICES

- Identity Management: CentOS 5 with Sun Identity Manager 8.1
- Key Escrow Service: StrongAUTH Strong Key Lite

2.1.4 SAMSON PROTECTION SERVICES

- SAMSON File Sharing PEP

- SAMSON Email PEP
- SAMSON Web Services PEP
- SAMSON Instant Message PEP
- SAMSON Policy Decision Point
- SAMSON Trusted Audit Server

2.2 FEATURES TESTED

The parameters for the trial scenario was well structured to effectively validate the following key features of SAMSON:

- Simultaneously view all caveats from a single work station.
- Inability to view unauthorized caveats,
- Inability to sign-on to unauthorized caveats After applying policy label and credentials,
- Within each of the caveats, ability to view all the files and directories on that level,
- Precluding access to levels for which warfighter did not have appropriate policy, labeland credentials,
- Ability to access caveated chat rooms based on policy , label and credentials,
- Ability to send and receive E mails based on policy, label and credentials,
- Ability to send and receive attachments to E Mails based on policy, label and credentials,
- Ability to re-label files and directories,
- Ability to access encrypted file data using authorized procedures,
- Inability to access encrypted file data to which the warfighter was not authorized to see,
- Ability to change a caveat on a file,
- Ability to create new policy,
- Ability to change existing policy,
- Acting as an Audit Security Officer, the ability to review the transactions logs for trusted audit chain verification,
- Acting as a Data Administrator, the ability to view all files and directories,
- Acting as a Data Administrator, the ability to move directories and create new directories,
- Acting as a Data Administrator, the ability to view the specific data on the files,

- Acting as a Data Administrator, the ability to delete files and directories; and
- Ability to access operational pictures by viewing Coalition Shared Database.(CSD) data
- Using Google Earth. The CSD is an existing information system product that holds image/video/data assets. DRDC built the piece to display CSD content via Google Earth and then added the SAMSON protection service to ensure that only those users that have the security policy right get to see those objects.

2.3 FEATURES NOT TESTED

At the time of execution, the developers reduced the scope of the demonstration such that the war fighters were not able to observe the following features of the technology

- Ability to create a new database,
- Ability to edit databases for which warfighter was entitled to access,
- Inability to edit databases for which warfighter was not entitled to access,
- Ability to create new database entries with metadata,
- Inability to create new database entries by using existing metadata for databases which warfighter was not entitled to access; and
- Ability to change a caveat on a data base entry

2.4 SCENARIOS

The CWID trial drew upon variation of the following scenario concepts which were integrated into the overarching CWID Master Event list for the entire week of CWID activities. A complete description of the events, objectives and role player actions are described in the CWID Master Scenario Event List (MSEL) Web Tool and use case documents.

1. A Colombian cargo ship, with several port destinations in Eastern Canada, approaches the port of St. John's and will head towards the St. Lawrence Seaway. There is intelligence information received from an RCMP intelligence officer that there may be contraband in the cargo on the ship coming from Columbia. At the MSOC meeting, some relevant intel about the Columbian vessel is revealed and discussed with relevant partners. Decision is made to create a new caveat for intel-sharing, and to track the ship. The Columbian vessel is nominated on the MEIL (Marine Entity of Interest List). It is decided at the meeting that the position of the ship (long, medium and short range) should be closely monitored by MSOC. And that additional information needs to be gathered on the cargo and crew list.
2. A Colombian cargo ship, with several port destinations in Eastern Canada, approaches the port of St. John's and will head towards the St. Lawrence Seaway. There is intelligence information received from an RCMP intelligence officer that there may be contraband in the cargo on the ship

coming from Columbia. The Administrator creates a new caveat for the event, adds caveats to the identity manager (assigns users)

3. A Colombian cargo ship, with several port destinations in Eastern Canada, approaches the port of St. John's and will head towards the St. Lawrence Seaway. There is intelligence information received from an RCMP intelligence officer that there may be contraband in the cargo on the ship coming from Columbia. The ship position is monitored by assets in the area

2.5 TEST INITIATION

The EC2011 configuration included two independent but connected SAMSON installations: SAMSON located in the Ottawa DRDC data center and SAMSON-AZ which was deployed to the operational site at Fort Huachuca. Connectivity between the two sites was provided by JFCOM through their dedicated EC2011 communications nexus in Arlington Virginia. Due to the sporadic nature of the connectivity between sites, the demo installations were able to operate independently, but share services when the connection was present. Workstations were co-located with each installation and connected directly to the SAMSON infrastructure.

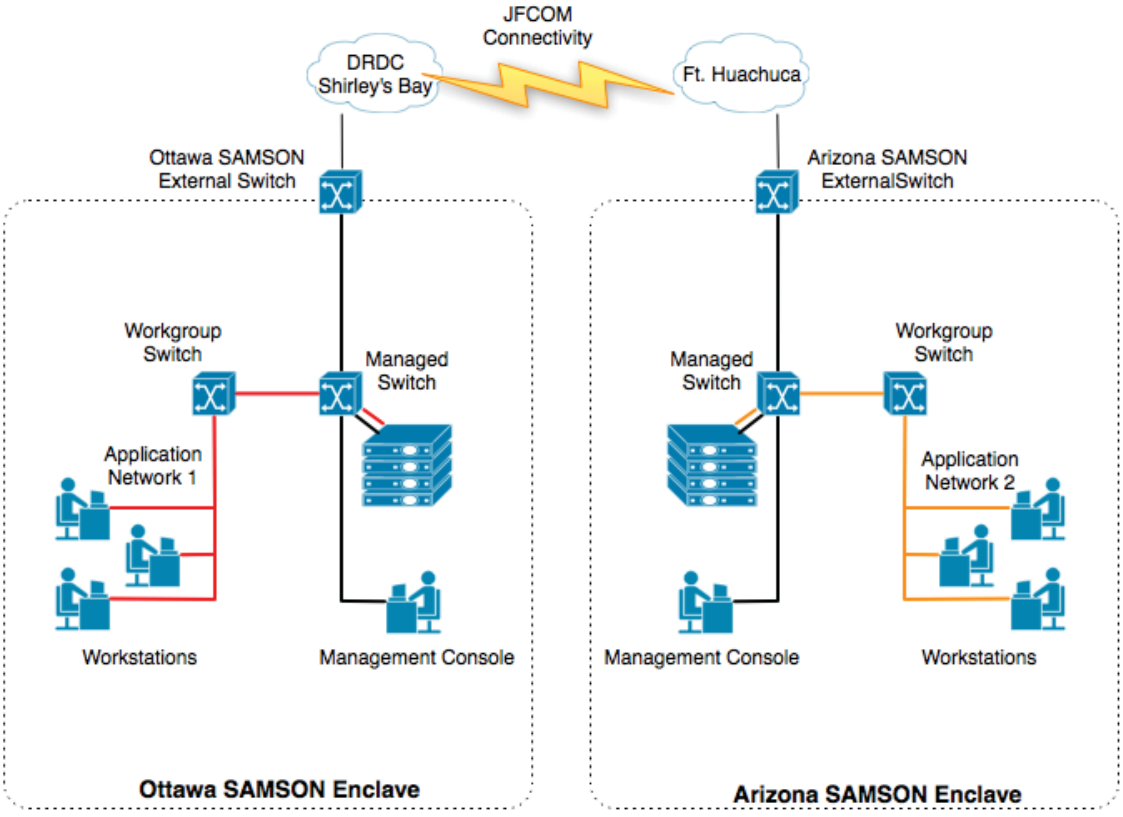


Figure 1 Empire Challenge 2011 Network Approach

The CWID configuration re-used the SAMSON installation from the EC2011 trial, but separated the primary operations workstations from the management console by

placing them on a separate network in a physically protected building. Workstations from the operations zone connected via the DRDC networking services to the SAMSON infrastructure over a VPN protected session.

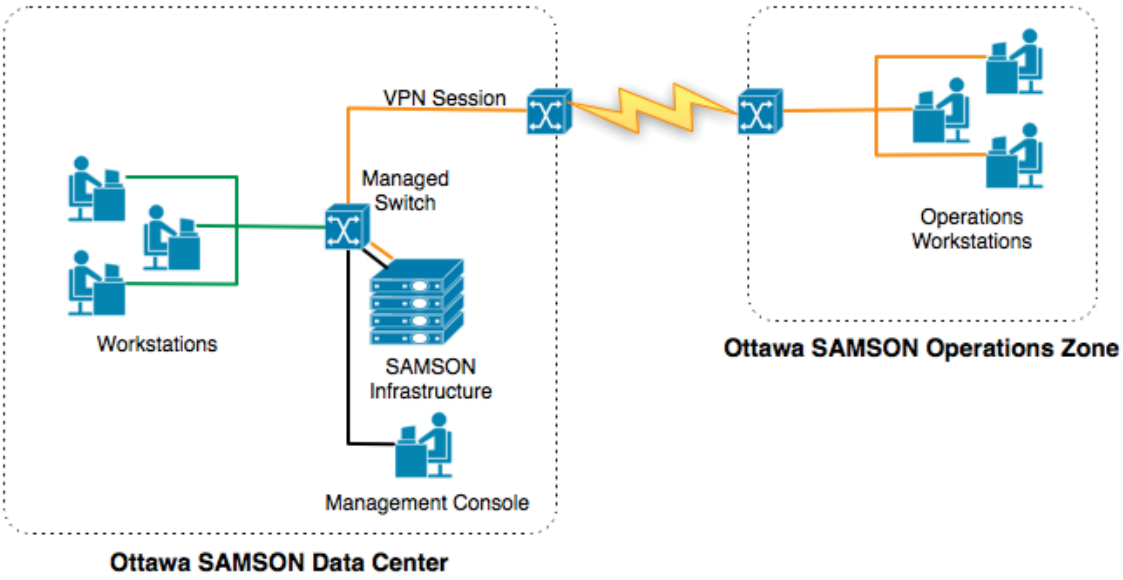


Figure 2 CWID 2011 Network Approach

2.6 PARTICIPANTS

Both trials included the following teams:

- Bell Canada: Glen Henderson, Brent Nordin, Bill Pase, Daniel Seguin
- DRDC: David Brown, Bruce Carruthers (contractor), Daniel Charlebois, Kathy Perrett, Darcy Simmelink

Additionally. the CWID trial included a Technical Assessor who performed the actual scenarios as defined by the CWID MSEL events and provided a report on SAMSON capabilities and responded to a questionnaire related to the assessment.

2.7 TASKS AND RESPONSIBILITIES

- Bell Canada: Trial Setup, Support and custom development
- DRDC: Execution of the EC2011 Trial scenarios and coordination and liaison between SAMSON, DND and the CWID organization
- Assessment Team: CWID trial execution and reporting

2.8 SET-UP AND FACILITIES

Both the EC2011 and CWID trials are described below in terms of the physical, network, virtual and component level configuration.

2.8.1 PHYSICAL SETUP

The Ottawa lab consisted of 2 Dell PowerEdge R600 blade servers running XenServer virtualization software. A third Dell PowerEdge (R415) hosted the StrongAuth Key Escrow Service. The SAMSON networks were segregated onto 4 separate VLANs hosted on a Dell PowerConnect managed switch. Three desktop machines were set up to be used as end user workstations and one workstation was set aside as a management console. An external Cisco switch connected the SAMSON infrastructure to the external DRDC/JFCOM networks and a Netgear firewall router bridged between the SAMSON and external networks.

The Arizona infrastructure consisted of 2 Dell PowerEdge R600 blade servers running XenServer virtualization software. A third Dell PowerEdge (R415) hosted the StrongAuth Key Escrow Service. The SAMSON networks were segregated onto 4 separate VLANs hosted on a Dell Power-Connect managed switch. Three laptops machines were set up to be used as end user workstations and one laptop was set aside as a management console. An external Cisco switch connected the SAMSON Arizona infrastructure to the external DRDC/JFCOM networks and a Netgear firewall router bridged between the SAMSON Arizona and external networks.

The CWID operations zone consisted of three desktop workstations configured with the SAMSON software baseline. This baseline included all workstation software components described in Section 2.1 Test Items. The machines and connectivity were provided by the CWID facilities group.

2.8.2 NETWORKING

The SAMSON infrastructure is deployed onto 4 core networks. Individual virtual machines connect to individual networks as required to fulfil their function. Each network is described below:

- Management: The management network is used to provide low-level system administration access to all machines. It is the point-of-entry network for all external connections to the infrastructure. Services hosted on this network include connectivity service such as VPN servers and common services used across all networks such as LDAP and DNS.
- Applications: The applications network is used as the operations network for business activity. The WIndows domain is hosted on this network and all workstations connect to this network in order to access domain services. Data services are hosted off this network and, therefore, policy enforcement points are similarly bound to this network. Security services such as the IDM are also hosted on this network.
- Security: The security network hosts the SAMSON Authorization server and the Key Escrow Server
- Aduit: The audit network hosts the SAMSON Trusted Audit Service and is only used to host audit traffic

There exists a firewall to bridge between networks, however, it is expected that this firewall is only used in exceptional cases. Where a server has a need to communicate on a particular network, that server should be attached to the network in question. For example, the File Server PEP has a need to communicate on all four networks: the management network for system administration purposes, the applications network to provide file sharing service to the workstations, the security network to

pose policy requests to the SAMSON infrastructure and the audit network to audit its actions. The guiding principles for the SAMSON deployment are, therefore: systems bind to networks on which they have a need to communicate, services are bound to specific interfaces (and therefore networks) and all unneeded services and network connections are disabled.

2.8.3 COMPONENT IDENTIFICATION

The SAMSON installation consists of XenServer 5.6 virtual machines based on one of two base templates:

1. Windows:Windows 2003 Server, 1GB memory, 8GB disk space (additional disk space added as needed)
2. Linux: CentOS 5.3 32-bit, 512MB memory 5GB disk space

The following table identifies the Virtual Machines that were instantiated into the SAMSON CWID installation, their template type and and indication as to whether they are part of the infrastructure (basic data services) or part of the SAMSON data protection services. This table also shows the networks to which the systems have been connected.

Table 1 SAMSON Virtual Machines and Network Participation

VM	Template	Type	Networks			
			Management	Application	Security	Audit
Active Directory	Windows	Infrastructure		X		
Exchange Server	Windows	Infrastructure		X		
File Server	Linux	Infrastructure	X	X		
CSD[1]	Windows	Infrastructure		X		
GCCS[2]	Linux	Infrastructure	X	X		
Identity Manager	Linux	Infrastructure	X	X		
SAMSON XMPP	Linux	SAMSON	X		X	
Trusted Audit Server	Linux	SAMSON	X			X
File and Web PEPs	Linux	SAMSON	X	X	X	X
Messaging PEPs	Linux	SAMSON	X	X	X	X
Authorization Server	Linux	SAMSON	X		X	X
IDM Gateway	Linux	SAMSON	X		X	X
Services[3]	Linux	Infrastructure	X	X	X	X

The following diagram shows the configuration elements in the SAMSON installation. The elements in blue indicate the original data services, that is, those services that existing and provided service before the infrastructure was protected with SAMSON. The elements in red indicate the SAMSON components that have been added to the

1
2
3

environment to protect the information at rest and in transit. The elements in yellow represent SAMSON Audit Components.

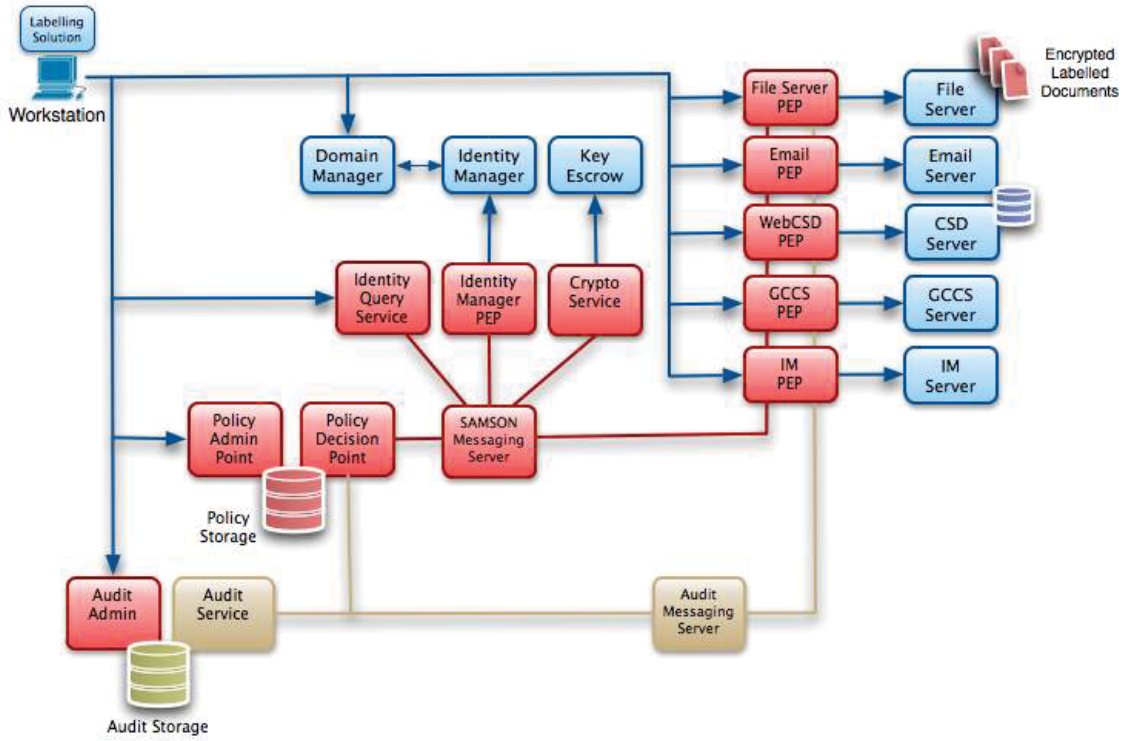


Figure 3 SAMSON Component Identifiers

The following table identifies the SAMSON component services that were instantiated into the SAMSON CWID installation and the networks to which the services have been bound.

Table 2 SAMSON Virtual Machines and Network Participation

Component	VM	Description	Networks			
			Management	Application	Security	Au
File Server PEP	File and Web PEPs	WebDav intercept		443	PM	P
Email PEP	Messaging PEPs	ProxSMTP intercept		10025	PM	P
WebCSD PEP	File and Web PEPs	External Web Filter		443	PM	P
GCCS PEP	File and Web PEPs	External Web Filter		443	PM	P
IM PEP	Messaging PEPs	Transverse IM Client Plugin		5222	PM	P
IQS	IDM Gateway	REST API		8008	PM	P

IDMPEP	IDM Gateway	Service Module			PM	P
Crypto Service	File and Web PEPs				PM/SOAP	P
PDP	Authorization Server				PM	P
Policy Admin Tool	Authorization Server			8008		
Trusted Audit Servcie	Trusted Audit Server					P
Audit Admin Tool	Trusted Audit Server			443		

2.9 METRICS

While the initial focus of SAMSON for CWID 2011 was a single SECRET network, interfaces in support of multi-level architectures were to be demonstrated for data exchanges and data security label rationalization. The SAMSON CWID trial was to demonstrate the applicability and extensibility of multi-caveat separation to cross domain data exchanges for web services where the SAMSON data labelling is compatible with coalition Metadata Specifications and the DoD Discovery Metadata Specification. DRDC isolated seven key components of SAMSON to form the sponsor defined requirements (SDR) for the CWID demonstration as follows.

1. Restrict access to caveated files and directories
2. Preclude access to levels for which users do not have appropriate policy, label and credentials
3. Use caveated chat rooms according to policy, label and credentials
4. Create, access and edit data bases according to accreditation
5. View data/information with Google Earth
6. Send and receive E mails based on policy, label, and credentials
7. Create, access, amend files and caveats according to policy label and credentials

2.10 NEEDS

The CWID exercise provided access to all needed data sources as part of the master scenario scheduling effort.

2.11 STAFFING AND TRAINING

DRDC provided two experienced operators to conduct the SAMSON trial at Shirleys Bay: an Air force pilot with 32 years of experience and an Army Communication specialist with 11 years of experience of which four years were as the G3 for the Army Reserve Communications Group.

In addition the New Zealand Liaison Officer shadowed the activities of the war fighters during the events. The two war fighters and the New Zealand LO received

training by the SAMSON developers during Training Week, at Shirleys Bay. Although they were not provided guidebooks, they did not consider this a major deterrent in the performance of the events. While a technician was on call, there was minimal need for the services as the application worked well throughout the nine day demonstration.

2.12 DATA CAPTURED DURING THE TRIAL

All data was confiscated or destroyed at the end of the trial as the trial environment was classified. Hardware assets were returned to the SAMSON team.

2.13 RESULTS

The Canadian CWID Technical Assessor reported that SAMSON employed information from standard formats such as databases, chat rooms, email, and geospatial information in order to demonstrate that the system cryptographically separated caveats at the data level to provide caveat separation on a single network. According to the Warfighter Assessments, the demonstration was well structured to effectively validate the following key features of SAMSON. In the words of one warfighterTechnical

> *The application of policy and caveats is fairly simple and SAMSON allowed me to view the files I was entitled to see. I can see that this (control of caveats and policies) could become an administrative burden in a large or complex network/operating environment.*

All warfighters agreed SAMSON was very easy to learn and use. Some salient warfighter comments concerning the technologies are as follows.

> *I think it worked very well for physical security and data integrity.*
>
> *SAMSON creates what I would call tear line reporting... good for protecting sources and maintaining need to know and need to hold policies and as a result, good for information sharing. I do think it works as battle manager or analytical system.*
>
> *This tool can be used as a COP and to enforce security policies and caveats.*

In the Assessment Questionnaire, it was noted that the aim of the trial was to demonstrate that SAMSON provides fast access to critical classified data residing on physically separated caveats on one network, while preserving integrity and security. In response to the question "*Did the trial fully meet its aim?*" the consensus was the technology worked very well and the demonstration was well done.

2.14 DISCUSSION AND COMMENTS ON THE TRIAL

The following is a aggregated set of notes from the Bell SAMSON team regarding the EC2011 and CWID trials. It also includes some thoughts on SAMSON phase II in general. From a pure deployment/operations perspective, our view is that the execution of the demonstrations was very successful. All targets that were within our ability to achieve were delivered and demonstrated. We were able to do a lot of on-

the-fly modifications to enhance the operators' experience and that is a testimony to the flexibility of the SAMSON approach.

1. The Bell team found it most interesting that the majority of the technical issues that were encountered were either: associated with connectivity between 34 and 104 (not a SAMSON issue) or were very quickly tracked down and resolved. The efforts in 2010-2011 to consolidate code and standardize on specific coding routines simplified the implementation and resulting in a much more supportable infrastructure. There were no unanswered technical questions at the end of the exercises.
2. It is obvious to the Bell team that we are all a little too close to the SAMSON approach and that makes it hard for us to anticipate what a new operator's reaction will be to environment. We may want to create a SAMSON user guide that explains what SAMSON is and what it is not. The confusion over the presentation of audit logs is a good example. SAMSON is back-end focussed and enables (but does not provide yet) the ability to do forensics.
3. The team believes all the technical directions on SAMSON phase II were correctly chosen and implemented. The selection of WebDAV for file sharing and StrongAuth for key escrow have led to a much improved SAMSON story.
4. Running separate, isolated SAMSON instantiations is always a project risk. We should investigate better way to ensure code is synchronized with a clear authoritative source.
5. In phase III, we should ensure we are more focussed on the SAMSON TD delivery target. In terms of future capabilities for phase III, here is a consolidated list.
    a. Mutually authenticated TLS between XMPP identities. We would need to use locally stored certificated to do this and we propose we leave the question of how to protect those certificates as an implementation detail (there are already ways to do this). XMPP servers support a CRL so we will also support cert revocation as a side-effect of doing mutually authenticated TLS
    b. Code cleanup issue: There is a new XMPP layer that is already in use at all the PMs. It must be integrated with the SAMSON security services, including:audit, pdp, and the idm gateway
    c.**Important**The XMPP layer should reconnect after network failure. Right now we need to restart pieces manually after a network failure. Similarly, we should handle initial connection failures in a better/more helpful manner. This one change would provide substantial stability improvements. Currently, SAMSON is stable, but requires restarts to recover from unexpected conditions. A re-connecting SAMSON XMPP layer (which is very much the intent of XMPP application design) would ensure that all SAMSON pieces can recover from an unexpected state.
    d. Bell suggests that SAMSON should have more advanced monitoring tools that have the ability to query endpoints (get status messages from things like the PDP). Obviously here we are talking about using XMPP to monitor itself. There is a range of status details from the PMs/GWs like uptime,query count, status of the backend service.

e. We need to improve our own logging to make it easier to diagnose issues. We should keep logging facilities separate (xmpp level, pm level, intercept level). We also should make sure that logging only contains non-sensitive information or at least has the ability to log at a level of detail that omits sensitive data. It should NOT be possible to derive the security policy based on observing the log files

f. What we are auditing needs to be revisited and rationalized. We recommend that we have a requirements gathering process for this at the beginning of phase III. Some brainstorming was done at bldg 34 and that can serve as the basis for the discussion.

g. An idea is to implement a Policy Information Point. This would be a service that exists in front of the actual PDP and is responsible for collecting all supplemental data that is needed by the PDP itself. Currently, our PDP does the PIP activities and separating them will bring SAMSON more in line with the XAMCL specification.

h. Similarly, we recommend a mechanism whereby all intercepts are coded with a very granular set of ACTIONS (for example a file server could have separately enforceable policy actions for file read, write, rename, delete, create, etc...) but that have the ability to maps granular actions to more general ones (e.g. rename = write). This saves us from having to keep updating the intercepts each time to achieve the desired level of granularity at the policy level.

i. Cryptographically bound labels are needed for phase III (note that this does not necessarily require PKI based signatures) This feature is already available in a limited fashion in SAMSON phase II but needs to be turned on and tested.

j. Need to revisit file locking in WebDAV and review the logging that is done for that intercept, however the approach for used for CWID worked quite well.

k. Bell suggests we drop Transverse once and for all and return to the Spark IM which provides SSO. SAMSON required strong authentication so all SAMSON pieces MUST be using the windows domain credential identity for policy decisions.

l. We need to decide for all other applications (that is, other than file sharing) what it means to protect the data at rest. Do we want to insist that persistent chat rooms are encrypted with a key from StrongAuth? Similar issues for email.

m. Exchange protocol support still required.

n. We should identify for each application type what is the targeted application. For example the CSD is our web service demonstration application. We should define this early in phase III so we all have a known end target in mind.

o. We should implement the SAMSON protected TCP port concept using RDP as the sample application (similar to the terminal services solution that was demoed at CWID except that SAMSON would be gating access to that RDP port.)

p. SAMSON database support. Do we target row level or column level security? The SAMSON phase I Oracle based solution worked quite well for row level security.

q. SELinux... we are using a security enhanced Linux distribution, but we are not enforcing security policies. Is that enough for a SAMSON TD, or do we want to spend the time developing the policies for the host. It is propose we put that activity with the hardening activities which MUST occur separately from the phase III development activities.

2.15 SOFTWARE VERSION CONTROL

Blade System	
XenServer	6.0.210
Samson VM Template	5.0
Management Console	
Windows	7
XenCenter	6
Workstations/Laptops	
Windows	7
Microsoft Office	2007
Titus Doc Classification	3.5
Titus Msg Classification	3.5
Transverse Client	1.5.2

ThirdParty	
Package	Version
Microsoft Active Directory	2008
Titus MS Office Plugin	3.5
AlienVault (SIEM)	4.1
Windows File Server	2008
StrongAuth SKLES	Build 50;Centos 5.5
MS Exchange	2007

Repository	
Package	Version
CENTOS	6.3
DNS Services (Dnsmasq)	2.63
OpenLDAP	2.4.34
Mysql	5.6.10

Security Messaging Server	
Package	Version
CENTOS	6.3
OpenFire	3.7.1

Audit Messaging Server	

Package	Version
CENTOS	6.3
OpenFire	3.7.1

Identity Attribute Service	
Package	Version
CENTOS	6.3
samsoncode.tar	439

Authorization Service (PDP Server)	
Package	Version
CENTOS	6.3
samsoncode.tar	439

KMS	
Package	Version
CENTOS	6.3
samsoncode.tar	439

Trusted Audit Service	
Package	Version
CENTOS	6.3
samsoncode.tar	439

PEP: File Share	
Package	Version
CENTOS	6.3
filepep.tar	430

PEP: Email	
Package	Version
CENTOS	6.3
emailpep.tar	430

PEP: IM Server	

Package	Version
CENTOS	5
im_pep.tar	430

PEP: Web Session Service	
Package	Version
CENTOS	6.3
websession.tar	430

2.16 ROLES AND RESPONSIBILITIES

Role	Sub-Role	Account Ownership	Responsibilities
Security Officer(SO)		N/A	Observes the installation activities undertaken by the System Administrator
System Administrator (SysAdmin)	all	XenServer Access	All System Administrators have access to the credentials for the XenServer virtualization platform
	installer	VM system root account	Configuration of the networking and application intercepts. Configuration of the startup process for the automated launch of services
		Repository Directory Server root account	Management of the directory server schema and individual organizational unit delegated accounts
		Repository Database root account	Management of database creation and individual database accounts
	manager	System account	Deployment and configuration of SAMSON services. Operational account under which all SAMSON processes run.
		XMPP admin accounts	The accounts (2) used to

Role	Sub-Role	Account Ownership	Responsibilities
			access the OpenFire administrative consoles
SAMSON Administrator (SamAdmin)	idmadmin	A SAMSON user account authenticated via Windows Domain authentication. The idmadmin sub-role is assigned by associating the IAAI_ADMIN caveat to that account.	When holding this caveat, the idmadmin has the policy right to administer SAMSON user caveats through the Identity Attribute Administrative Interface.
	policyadmin	A SAMSON user account authenticated via Windows Domain authentication. The policyadmin sub-role is assigned by associating the PAI_ADMIN caveat to that account.	When holding this caveat, the policyadmin has the policy right to administer SAMSON policies through the Policy Administrative Interface.
	auditadmin	A SAMSON user account authenticated via Windows Domain authentication. The auditadmin sub-role is assigned by associating the ARI_ADMIN caveat to that account.	When holding this caveat, the auditadmin has the policy right to a view SAMSON audit records through the Audit Review Interface.

2.17 INSTALLATION AND CONFIGURATION TESTS

A time to complete the installation and configuration acitivities is provided in the table below. This estimate (9 hours) is based on an installer having a thorough knowledge of the Samson system, strong Centos linux skills, and a solid understanding of the tcp/ip network configurations of Centos VMs in an XenServer environment. If the installer does not have these skill sets, then the time to install could increase substantially. [Note: previous installation experience on complex crypto systems, consisting of four server machines, which make use of one database, one LDAP Directory, and a high number of configuration files requiring modifications can take up to 3 days with a full set of production grade documentation. The Samson system has two databases, one ldap directory, eleven server machines, and many configuration files which need modification. It could take from 22.5 hours up to 37.5 hours for an installer with less experience to install successfully a Samson system from bare metal machines.]

It is assumed that the Test Activities 1.0, 2.0 and 3.0 will be carried out by the hosting organization (CTDC) and no time estimates are provided.

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
1.0	**Preparation**		
1.1	Ensure that 2 Blade Servers for the XenServer hypervisors are available.		Pass
1.2	XenServer is installed on the Blade		Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
	Servers		
1.3	A XenCenter is installed on a machine and is available and configured to permit control of the XenServer machines.		Pass
1.4	A Samson VM Template is available with all the software required to complete the install and configuration process.		Pass
1.5	The Samson Deployment and Configuration document latest version is available.		Pass
2.0	**Target Environment Preparation**		
2.1	There is an Active Directory system present in the target environment with a specific OU for Samson.		Pass
2.2	The user workstations/laptops used in the SAMSON environment are joined to the Windows domain		Pass
2.3	A set of user accounts have been set up in the domain?		Pass
2.4	Within the domain, SAMSON has use of one of the AD extensionAttribute schema values associated with domain users		Pass
2.5	Individual user workstations/laptops have the Titus 3.5 labelling software (Document and Message labelling plus-ins for Microsoft Office) installed and the Titus software has been configured to use the extensionAttribute value for AD queries?		Pass
2.6	File Sharing: A Microsoft File and Print Sharing file share is present? A separate domain account has been created with read/write privilege on this file share for Samson Users.		Pass
2.7	Email: An SMTP/POP3 based mail server is present in the environment. The SMTP and POP3 services have been enabled.		Pass
2.8	Instant Messaging: An IM server with chatrooms is present in the environment		Pass
2.9	The IM server is using the Windows domain for its user account base and a separate domain account called “spectrum” has been established for the domain.		Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
3.0	**Samson Hardware Preparation**		
3.1	The 2 Blade servers are available with: dual quad core processors (8 cores), 16GBRAM 4 physical NICs 160GB storage		Pass
3.2	A 24-port Managed Switch is available and configured with four 6 port VLANs (MGMT network, DATA network, SECURITY network, and AUDIT network.)		Pass
3.3	3 desktop/laptop systems are available? (1 for the management console (on the MGMT network)); (2 for domain workstations (on the DATA network))		Pass
3.4	Is a StrongAuth appliance available		Fail
3.5	Alternate Crypto Database is available for installation (if StrongAuth is not available)?		Pass
3.6	All required Hardware is available as per Section 3.2.1 of the Deployment and Configuration Guide?		Pass
3.7	Checklist of Configuration Elements has been completed	60 min	Pass
3.8	Define IP Addresses for each Machine and complete the Machine Network Configuration Table	30 min	Pass
4.0	**Creating Samson Machines**		
4.1	Has a VM on the XenServer been created by the “installer” from the VM Template (as per Section 4.2.1 of the Deployment and Configuration Guide)?	15 min	Pass
4.2	Has the Networking for the VM been configured by the “installer” as per Section 4.2.2 of the Deployment and Configuration Guide?	10 min	Pass
5.0	Repository Machine		
5.1	Has the Repository Virtual Machine been created by the “installer” as per Section 5.1 of the Deployment and Configuration Guide?	30 min	Pass
5.2	Have the MySQL, OpenLDAP, and the DNS Services been started by the “installer”?	5 min	Pass
6.0	Security Machine		
6.1	Has the Security Machine been	15 min	Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
	created by the "installer" and configured as per Section 5.2 of the Deployment and Configuration Guide?		
6.2	Is the Security Machine listening on ports 5222, 5223, and 9091		Pass
7.0	Audit Machine		
7.1	Has the Audit Machine been created by the "installer" and configured as per Section 5.3 of the Deployment and Configuration Guide?	10 min	Pass
7.2	Is the Audit Machine listening on ports 5222, 5223, and 9091		Pass
8.0	Security Gateways		
8.1	Has an Identity Attribute Machine been created by the "installer" as per Section 6.1 of the Deployment and Configuration Guide?	30 min	Pass
8.2	Has an Authorization Machine been created by the "installer" as per Section 6.2 of the Deployment and Configuration Guide?	10 min	Pass
8.3	Has the Key Management Machine been created by the "installer" as per Section 6.3 of the Deployment and Configuration Guide?	10 min	Pass
8.4	Option 1:Using local key storage (6.3.1) Option 2:Using StrongAuth (6.3.2)	10 min (Option 1)	Pass
8.5	Has the Trusted Audit Machine been created by the "installer" as per Section 6.4 of the Deployment and Configuration Guide?	5 min	Pass
8.6	Has a PEP been created by the "installer" with a dispatcher installed as per Section 7.1 of the Deployment and Configuration Guide?	10 min	Pass
8.7	Verify the Dispatcher Testing has been carried out successfully by the "installer" as per Section 7.1.2 of the Deployment and Configuration Guide?	15 min	Pass
8.8	Has a File Service PEP been created successfully by the "installer" as per Section 7.2 of the Deployment and Configuration Guide?	15 min	Pass
8.9	Has an Email PEP been created successfully by the "installer" as per Section 7.3 of the Deployment and Configuration Guide?	15 min	Pass
8.11	Has an IM PEP been created	15 min	Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
	successfully by the “installer“ as per Section 7.4 of the Deployment and Configuration Guide?		
8.12	Has a Web Session PEP been created successfully by the “installer“ as per Section 7.5 of the Deployment and Configuration Guide?	60 min	Pass
8.13	Were the Samson Web Services certificates generated and installed successfully by the “installer“ as per Section 7.5.1 of the Deployment and Configuration Guide?	15 min	Pass
	Total Time = Complete system setup + Creating each machine * 10 (Section 4.2.1 and Section 4.2.2)	295 min (4 hours 55 mins) + 250 min (4 hrs 10 min) Total Setup Time = 9hrs 5 min	

3 FUNCTIONAL TESTS

The activities associated with the conducting of the Functional Tests are provided in this section.

3.1 FUNCTIONAL TESTS PREPARATION

Test Activity No.	Test Preparation	Roles	Time	Pass/Fail (Yes/No)
	As the "manager" establish a number of Samson test users in AD	manager	10 min	Pass
	Establish a number of Samson test users in the Samson Directory Server	idmadmin	5 min	Pass
	Assign caveats to the Samson test users in the Directory Server	idmadmin	5 min	Pass
	Develop Samson Policies to be used in the functional tests	policydmin	10 min	Pass
	As a Samson user create a number of Word documents on the protected File Server with various caveat designations.	Samson User	15 min	Pass
	Carry out the functional tests for File Services	All	20 min	Pass

3.2 FILE SERVICES FUNCTIONAL TESTS & RESULTS

3.2.1 TESTS & RESULTS - FILE SERVICES

Control end user access and functionality to file resources (Microsoft Word documents) on a common file server using the users and resource assigned caveats in conjunction with established SAMSON Policy rules.

3.2.2 SPECIAL REQUIREMENTS

Four users were set up within the IDM system, by the "idmadmin", with the caveats as indicated:

TestUser1 (ottawa) caveat=ceo

TestUser2 (toronto) caveat=ceo, canus

TestUser3 (chicago) caveat=ceo,canus

TestUser4, (newyork) caveat=canus.

Policies were controlled by a "policyadmin" and audit records were viewed by the "auditadmin".

The Titus plugin and interface to Microsoft Word 2007 was used to select user assigned caveats to the resources.

3.2.3 ASSUMPTIONS

Users are authenticated by the Microsoft Active Directory. Windows Explorer was used to access the resources on the File Server. The testing was carried out on file level resources not at the folder level.

3.2.4 USER INTERFACE

In normal use, SAMSON users will access the file server through Windows 7, Windows Explorer file manager application, and the Microsoft Word 2007 application

SAMSON Policies will prevent users from seeing the existence of files to which they are not in the Community of Interest (ceo and/or canus) entitled.

3.2.5 INSTALLATION AND SETUP

Through the windows File Server mapped network drive there is one folder called "data" that the test user will obtain access to by logging into using their Windows AD account.

The data folder was populated with a number of user Word documents and based on the users assigned caveats – caveats were attached to the Word document;

3.2.6 ASSURANCE

Assurance that the SAMSON services are performing in accordance with the user and file objects assigned caveats and the authorization policy rules, was confirmed by the "auditadmin" reviewing the Audit records for the transcations.

3.2.7 TEST COVERAGE MATRIX

Userid	Policy Actions	Nationality	UserCaveat	Clearance	Resource Caveat	Result (Pass/Fail)
other1	user is denied all access	other	none	secret	ceo,canus	Pass
ottawa	user has read only access to resources labelled ceo	can	ceo	secret	ceo	Pass
ottawa	user has full access to ceo; no access to canus	can	ceo	secret	ceo	Pass
newyork	user has no access to ceo; read only access to canus	can	canus	secret	canus	
toronto	user has read only access to ceo and canus	can	canus,ceo	secret	canus,ceo	
chicago	user has full access to ceo; read only access to canus	can	ceo,canus	secret	canus,ceo	
newyork	user has no access to ceo; full access to canus	us	canus	secret	canus	
chicago	user has full access to canus; read access to ceo	us	canus,ceo	secret	canus,ceo	
toronto	user has full access to ceo and canus	can	canus,ceo	secret	canus,ceo	

3.3 INSTANT MESSAGING TESTS & RESULTS

3.3.1 OBJECTIVE

Instant Messaging (IM) testing was carried out only on the IM Client to Server;

The IM Client to Server component was tested by setting up a conference room and ensuring that:

- specific users can enter a conference room, which has been assigned a specific caveat;
- other users can join the conference room;
- be denied access to the conference room; or
- unable to see the plain text messages between Samson protected users.

3.3.2 TEST COVERAGE MATRIX:

The test cases explored combinations of valid and invalid boundary values for conditions being tested.

All user interfaces were through the TransVerse IM client application.

The following users, policies and caveats were used for the IM Services:

Users: ottawa, georgew, johna

Policies: CEO,(read, write); CANUS,(read,write)

Conference Room Caveats: CEO or CANUS

Marked-Up Conference Room Caveats: CEO or CANUS

Results: Rx=user received; tx= user transmits; tx(ceo) [indicates a Marked Up CEO caveat multi-user conference]; no msg indicates that the users chat room window displayed no message.

The Instant Messaging application services test matrix is as follows:

Chat Room Caveat (ceotestroom1)	user1	policy	user1 idm caveats	user2	user2 policy	user2 idm caveats	user3	user3 policy	usr3 idm caveats	Result
Ceo	georgew	ceo,canus	canus	ottawa	ceo,canus	ceo	johna	ceo,canus	ceo,canus	
	Action	Result		Action	Result		Action	Result		
	tx	rx			rx			rx		
		rx		tx	rx			rx		
		rx			rx		tx	rx		
	tx(canus)	rx			rx			rx		
		rx		tx(canus)	rx			rx		
		rx			rx		tx(canus)	rx		
	tx(ceo)	rx			rx			rx		
		rx		tx(ceo)	rx			rx		
		rx			rx		tx(ceo)	rx		

3.4 EMAIL TESTS & RESULTS

3.4.1 OBJECTIVES

The E-Mail Messaging Tests were carried out to validate the capability of the SAMSON TD system to:

Control access to Outlook client message sender and recipients to E-Mail service resources on a Microsoft Exchange Server 2007 SP1 using the sender/recipient users and message resources with attachments, with assigned caveats in conjunction with established SAMSON Policy rules.

3.4.2 SPECIAL REQUIREMENTS

Four users were set up within the IDM system with the caveats as indicated:

TestUser1 (ottawa) caveat=ceo,canus

TestUser2 (chicago) caveat=ceco,canus

TestUser3 (toronto) caveat=ceo,canus

TestUser4 (newyork) caveat=ceo,canus

Policies were controlled by the "policyadmin" and audit records were viewed by the "auditadmin".

The Titus plugin and interface to Microsoft Outlook Client 2007 was used to select user assigned caveats to the message resources.

3.4.3 ASSUMPTIONS

Users were authenticated by the Microsoft Active Directory. Files used for attachments were stored in the SAMSON Windows File server data folder under "at rest" encryption protection. The testing was carried out on messages with no attachments.

3.4.4 USER INTERFACE

In normal use, SAMSON users access the E-Mail Services through Windows 7, Microsoft Outlook Client, and the Titus Trusted Labelling Service provides the message caveats available to the sender through the Outlook Client application.

SAMSON Policies prevent senders attaching files within the Windows File Server data folder, to which they are not in the Community of Interest (ceo and/or canus).

3.4.5 E-MAIL – FUNCTIONAL TESTS AND RESULTS

Single Sender to Single Recipient – No attachments

Test Case #	Sender	Sender	Sender	Recipient	Recipient	Msg	Attachment	PDP Decision	Results
	name	idm caveat	policy	name	policy	caveat		permit	Pass/Fail
1	toronto	ceo,canus	ceo	chicago	ceo	ceo	none	**y**	msg delivered to sender
2	toronto	ceo,canus	ceo	Chicago	ceo	canus	none	n	sender policy violation canus recipient cannot receive ceo msg
3	toronto	ceo,canus	ceo	Chicago	canus	ceo	none	n	
4	toronto	ceo,canus	ceo	chicago	canus	canus	none	n	
5	chicago	canus	canus	toronto	ceo	ceo	none	n	sender chicago with an idm caveat of canus only; cannot select msg with a ceo caveat
6	chicago	canus	canus	tormto	ceo	canus	none	n	
7	chicago	canus	canus	toronto	canus	ceo	none	n	sender chicago with an idm caveat of canus only; cannot select msg with a ceo caveat
8	chicago	canus	canus	toronto	canus	canus	none	**y**	

4 NON FUNCTIONAL TESTS

4.1 PERFORMANCE

The objectives for performance of resources will be met by the generation of system input loads emulating systems type input conditions and the measurement of processes related to the input conditions, in terms of throughput, response times and utilization of resources. This will be augmented, where appropriate, by the use of modeling techniques to assist in determining the scaling requirements of Samson infrastructure components. This combination of actual measurements and modeling techniques will produce results, which will assist CTDC Engineers/Architects to provide cost effective solutions.

The performance tests will determine the storage capacity required for audit records.

4.2 MODELLING

The use of modeling techniques to predict or estimate performance, and scalability will be used.

4.3 TYPES OF TESTS

The types of non functional tests conducted will be:

Performance Testing – This type of testing collects data in terms of throughput, response times and utilization i.e. the number of transactions per second (TPS) and the transaction response time (TRT) (average/median/90 percentile, minimum, maximum,) the system can deliver over a range of system loads, measured by average percentage CPU utilization.

The performance tests will be carried out using a number of clients, up to 5, to provide the level of concurrency. The output will be measured for transaction response time and throughput with up to the 5 users concurrently carrying out transactions. An average throughput for the operation will be recorded. This test scenario will provide an indication of performance metrics, which can be used to calculate the maximum number of users that can carry out the specific process at the same time before the configuration requires additional resources or reconfiguration. The performance metrics will be tabulated in the format shown in the table below.

Number of Clients	CPU (%age util)	Average Response Time (milliseconds)	Throughput (users /sec)
1			
3			
5			

4.4 PERFORMANCE TEST RESULTS

4.4.1 EMAIL

An email message Python test tool was developed to generate user send SMTP traffic, and a user retrieve POP call. Two sets of performance numbers were collected one with no Samson email components in the system message flow and the other with the Samson email PEP in the system message flow. This provided an indication of the Samson email PEP overhead. The tests were conducted with no attachments, with a 250Kbyte attachment and

with a 850Kbyte attachment to determine the impact of attachment size on the Samson email PEP.

The results in terms of throughput (messages per second) and response time for each message (seconds per message) are provided in the following tables.

No Samson Email PEP in the Message Flow

total msgs sent or retrieved	Msgs per user	Users	Attachment Size	Time (secs)	protocol	Throughput (msgs/sec)	Response time per msg (secs/msg)
25	25	1		0.43	smtp	58.14	0.02
75	25	3		1.48	smtp	50.68	0.02
125	25	5		1.88	smtp	66.49	0.02
25	25	1	250KB	2.11	smtp	11.85	0.08
75	25	3	250KB	3.98	smtp	18.84	0.05
125	25	5	250KB	6.98	smtp	17.91	0.06
25	25	1	850KB	6.17	smtp	4.05	0.25
75	25	3	850KB	11.64	smtp	6.44	0.16
125	25	5	850KB	20.49	smtp	6.10	0.16
25	25	1		0.14	pop	178.57	0.01
225	25	3		1.12	pop	200.89	0.00
625	25	5		2.36	pop	264.83	0.00
25	25	1	250KB	1.78	pop	14.04	0.07
225	25	3	250KB	8.01	pop	28.09	0.04
625	25	5	250KB	18.35	pop	34.06	0.03
25	25	1	850KB	5.83	pop	4.29	0.23
225	25	3	850KB	23.57	pop	9.55	0.10
625	25	5	850KB	52.21	pop	11.97	0.08

With the Samson Email PEP

total msg	Msg/user	Users	Attachment Size	Time (secs)	protocol	CPU (%age)	Disk (blk/sec)	msgs/sec	secs/msg
25	25	1		163	smtp	16.7	345	0.15	6.52
75	25	3		207	smtp	21.51	584	0.36	2.76
125	25	5		259	smtp	25.28	900	0.48	2.07
25	25	1	250KB	209	smtp	18.74	1165	0.12	8.36
75	25	3	250KB	309	smtp	24.61	3049	0.24	4.12
125	25	5	250KB	410	smtp	31.44	7123	0.30	3.28
25	25	1	850KB	217	smtp	19.65	3578	0.12	8.68
75	25	3	850KB	319	smtp	31.25	27593	0.24	4.25
	25	5	850KB		smtp				
25	25	1		103	pop	16.6	122	0.24	4.12
225	25	3		310	pop	23.39	334	0.73	1.38
625	25	5		520	pop	31.32	3173	1.20	0.83

25	25	1	250KB	121	pop	18.97	1410	0.21	4.84
225	25	3	250KB	333	pop	32.47	4059	0.68	1.48
625	25	5	250KB	563	pop	42.23	23368	1.11	0.90
25	25	1	850KB	124	pop	24.2	20159	0.20	4.96
225	25	3	850KB		pop				
625	25	5	850KB		pop				

The results indicate that with one user sending an email with no attachments, without a Samson email PEP in the message flow, it takes 0.02 secs to send the message and 0.01 secs to retrieve the message. With the Samson Email PEP active in the message flow, with one user and no attachments it takes 6.52 secs to send the message and 4.12 secs to retrieve the message.

The email message throughput graph, Figure 4, indicates the throughput rate of the email system when the Samson email PEP is intercepting the traffic. A trendline is shown with a 250KB attachment, which indicates that approximately 20 concurrent users would generate a throughout rate of approximately 0.5 message per second. On the single CPU virtualized email PEP server, the maximum CPU utilization achieved was just over 30%.

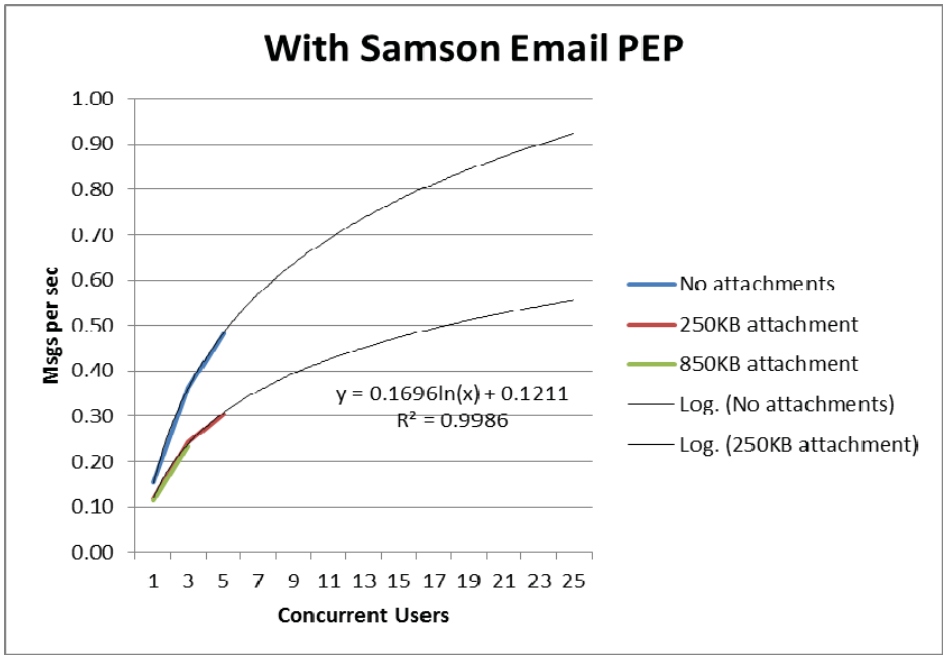
Based on the Microsoft MAPI Messaging Benchmark (MMB3) Model for the Exchange Server: Each user will send 84 messages per 8 hour work day with an average size message size of 74.9KB. Based on this, the number of users that can be supported by a Microsoft Exchange Server integrated with Samson, with a message throughput rate of 0.5 messages per second is:

Messages per day = 0.5 * 8 * 60 * 60 = 14,400 msgs per day;

Number of users = 14,400/84 = 171 users

The current configuration of the Samson Email environment will support up to 171 Outlook users, as outlined in the Email test results and calulations.

Figure 4: Email Throughput with the Samson Email PEP



Further, using an Email Message Throughput rate of 0.5 email per second (30 emails per minute), the user community size, number of active users, and session time can be calculated from the model:

Email Msg Throughput = (Total Number of Users * %age Active Users)/Session Time

The Email performance test results show that the Samson Email Services will support a user community size of 1000 users, where 150 are active in sending and receiving an email every 5 minutes.

It should be recognized that the current DRDC5 test environment is scaled as an entry level system, with minimum CPU and memory allocation per virtualized server.

The metrics obtained indicate that the introduction of the Samson email PEP and services can introduce an overhead of up to 8 seconds per message. This is without any tuning of the system. The Samson Email PEP and associated backend services are very busy carrying out:

- the intercept to obtain a copy of the message;
- decoding the message to get the attachments;
- starting a dispatcher for this transaction;
- carrying out the policy check;
- generating a new key and storing it;
- retrieving that key;
- carrying out the encryption;
- re-encoding and re-wrapping the new encrypted email;
- getting the intercept to re-read the new message and send it off to the server; and
- generating an audit record.

Future development activity should address the efficiency of this workload, for example having a number of dispatchers established in a "pool" eliminating a dispatcher start up cost, more efficient cryptographic key generation and management, etc.

4.4.2 INSTANT MESSAGING

A Python Instant Messaging (IM) test tool was developed to generate multiple user chat messages to a Samson protected chatroom with multiple Samson users resident in the chatroom. Two sets of performance numbers were collected one with no Samson IM components in the chat message flow and the other with the Samson IM PEP in the chat message flow. This provided an indication of the Samson IM PEP overhead. The tests were conducted with all users generating 500 chats, with no think time or user keyboard time. The time taken from the start of the first chat message being sent to the last chat message received was recorded.

The results in terms of throughput (chats per second) and response time for each chat (seconds per message) are provided in the following tables.

No Samson IM PEP

Total No of chat msgs sent & received	Chats per user sent	Clients	Time (secs)	Chats per sec	Secs per chat
1500	500	2	20.9	72	0.01
2000	500	3	21.3	94	0.01
3000	500	5	21.7	138	0.01

With the Samson IM PEP

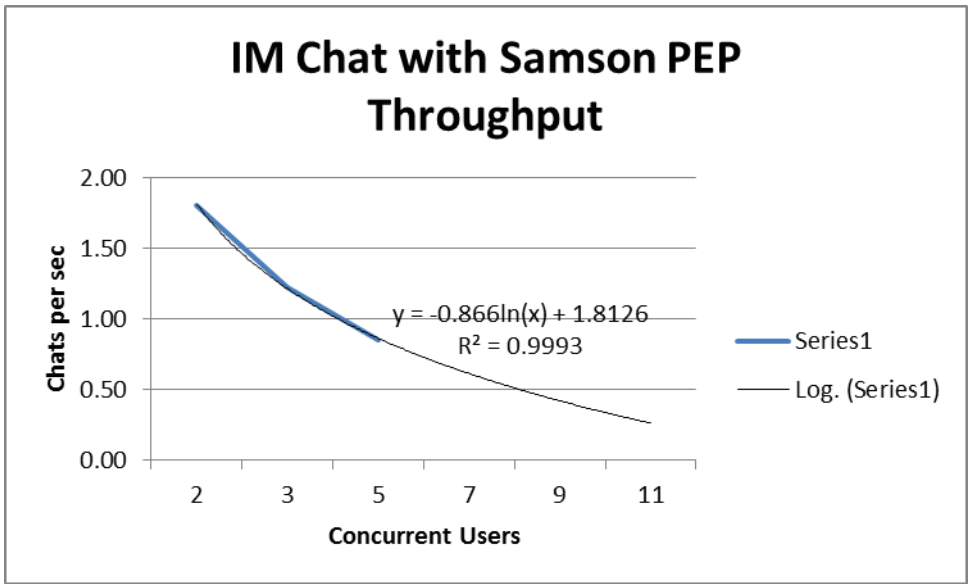
Total No of chat msgs sent & received	Chats per user sent	Clients	Time (secs)	CPU (%age)	Disk (blks/sec)	Chats per sec	Secs per chat
1500	500	2	830	16.24	973	1.81	0.55
2000	500	3	1630	12.77	1890	1.23	0.82
3000	500	5	3520	19.37	1058	0.85	1.17

The results indicate that with 5 users, a throughput rate of 0.85 chats per second or 51 chat messages per minute can be sustained. Using a Chat Throughput rate of 50 chat messages a minute the user community size, number of active users, and chat session time can be calculated from the model:

Chat Throughput = (Total Number of Users * %age Active Users)/Chat Session Time

Based on the test results and model calculations the Samson IM PEP can support a user community of 1000, where 150 are active and carrying out a chat session every 20 seconds.

Figure 5: Samson IM Throughput



The shape of the graph in Figure 5 indicates that the IM system with the Samson IM PEP is not scaling effectively. An investigation into this revealed that the Spectrum package used as part of the IM PEP was not configured to handle the type of load that was being generated by the test tool. The Spectrum configuration was modified to provide proof of this assertion. In addition, it was found that using the StrongAuth Key Escrow appliance was causing a considerable delay. Future development work should focus on these issues within the IM environment.

4.4.3 FILE SERVICES

A File Services Python test tool was developed to carry out an upload and download of Samson protected files from the mounted drive to a local drive. Two sets of performance numbers were collected one with no Samson file services components in the file transfer flow and the other with the Samson File Services PEP in the file transfer flow. This provided an indication of the Samson File Services PEP overhead. The tests were conducted with 1MByte files.

The results in terms of throughput (files per second) and response time for each file transfer (seconds per message) are provided in the following charts.

No Samson File Services PEP

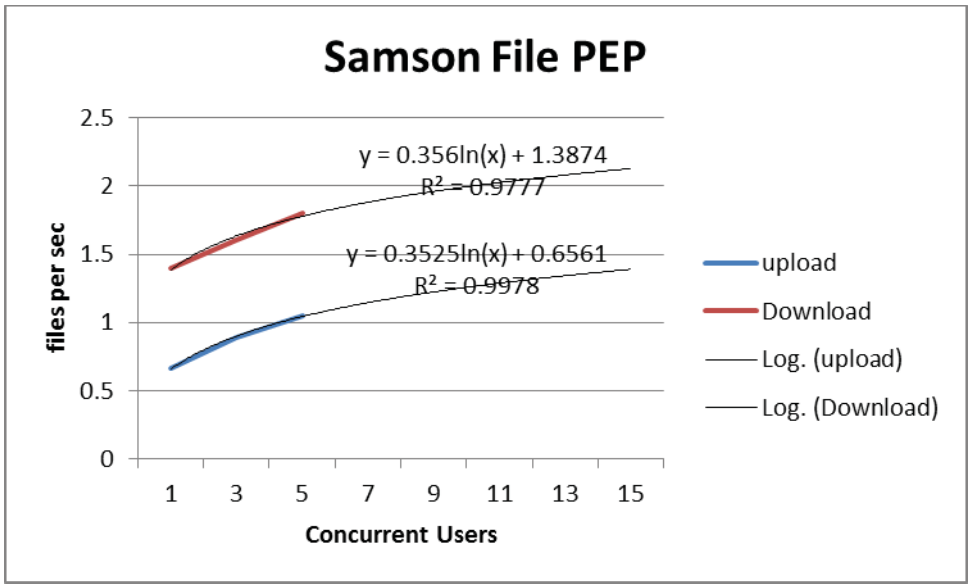
Files	Clients	Time (secs)	File Size	Upload/Download	Throughput (files/sec)	Response Time (Sec/file)
50	1	3.2	1MB	Upload	15	0.064
50	3	7.9	1MB	Upload	19	0.158
50	5	16.1	1MB	Upload	16	0.322
50	1	5.8	1MB	Download	9	0.116
50	3	18.1	1MB	Download	8	0.362
50	5	25.2	1MB	Download	9	0.504

With Samson File Services PEP

Files	Clients	Time (secs)	File Size	Upload/Download	Throughput (files/sec)	Response Time (Sec/file)
50	1	76	1MB	Upload	0.66	0.66
50	3	169	1MB	Upload	0.89	0.30
50	5	239	1MB	Upload	1.05	0.21
50	1	35.7	1MB	Download	1.4	1.40
50	3	92	1MB	Download	1.6	0.54
50	5	138	1MB	Download	1.8	0.36

As shown in Figure 6 below the results can be extrapolated to show that, an average file transfer (upload or download) throughput rate of 1.5 files per second (90 files per min), for 10 concurrent users, can be achieved by the Samson File Services.

Figure 6: Samson File Services Throughput



Using a File Transfer (Upload/Download) Throughput rate of 90 files per minute the user community size, number of active users, and session time can be calculated from the model:

File Transfer Throughput = (Total Number of Users * %age Active Users)/Session Time

The file transfer performance test results show that the Samson File Services will support a user community size of 1000 users, where 400 are active in transferring (uploading or downloading) a 1 MByte file every 5 minutes.